**Date: September 9, 2026**

| Revision | Date | Changes |
|---|---|---|
| 1.0 | September 9, 2026 | Initial release |

The CVE-ID tracking this issue: CVE-2026-2380
CVSSv3.1 Base Score: 7.4 (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L)
CVSSv4.0 Base Score: 5.1
(CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:P/VC:N/VI:N/VA:N/SC:L/SI:L/SA:L)
Common Weakness Enumeration: CWE-256: Plaintext Storage of a Password
This vulnerability is being tracked by BUG 1207374

# Description

On affected platforms running Arista EOS with OpenConfig-related services (i.e., gNMI, gNSI, RESTCONF and NETCONF), sensitive requests and responses may be unintentionally logged. These may be stored on the local EOS device or recorded on remote accounting servers. Note that gRPC-based streaming via Streaming Telemetry Agent to CloudVision is not affected by this vulnerability.

Examples of sensitive information include:

- Sensitive CLI commands (e.g., “username bob secret myPass”)
- Sensitive OpenConfig YANG leafs (e.g., “system/aaa/global/tacacs/config/secret-key”)

This issue was discovered internally by Arista, and the company is not aware of any malicious exploitation of this vulnerability in customer networks.

# Vulnerability Assessment

## Platform and Software Applicability Note

To determine actual exposure, operators should first check their software versions against the "Affected Software" list below. If your software release is not listed, your deployment is not vulnerable, regardless of the hardware platform in use.

## Affected Software

### EOS Versions

- 4.36.1F and below releases in the 4.36.x train
- All releases in the 4.35.x train
- All releases in the 4.34.x train

- All releases in the 4.33.x train
- All prior releases

## Affected Platforms

The following products **are** affected by this vulnerability:

- Arista EOS-based products:
  - 710 Series
  - 720D Series
  - 720XP/722XPM Series
  - 750X Series
  - 7010TX Series
  - 7020R/R4 Series
  - 7130 Series running EOS
  - 7170 Series
  - 7050X3/X4 Series
  - 7060X/X2/X4/X5/X6 Series
  - 7260X/X3 Series
  - 7280R/R2/R3/R4 Series
  - 7300X/X3 Series
  - 7320X Series
  - 7358X4 Series
  - 7368X4 Series
  - 7388X5 Series
  - 7500R/R2/R3 Series
  - 7800R3/R4 Series
  - 7700R4 Series
  - AWE 5000 Series
  - AWE 7200R Series
  - CloudEOS
  - cEOS-lab
  - vEOS-lab
  - CloudVision eXchange, virtual or physical appliance

The following product versions and platforms **are not** affected by this vulnerability:

- WI-FI Arista Wireless Access Points
- CloudVision CUE, virtual appliance or physical appliance
- CloudVision CUE cloud service delivery
- CloudVision Portal, virtual appliance or physical appliance
- CloudVision Appliance Software
- CloudVision as-a-Service
- CloudVision AGNI - Cloud service delivery
- CloudVision AGNI - Virtual or physical appliance

- Arista 7130 Systems running MOS
- Arista Converged Cloud Fabric (formerly Big Switch BCF)
- DANZ Monitoring Fabric (DMF) - Controller Appliance
- DANZ Monitoring Fabric (DMF) - Analytics Node Appliance
- DANZ Monitoring Fabric (DMF) - Recorder Node Appliance
- DANZ Monitoring Fabric (DMF) - Service Node Appliance
- Arista Multi Cloud Director (formerly Big Switch MCD)
- Arista Network Detection and Response (NDR) Security Platform (Formerly Awake NDR)
- Arista Edge Threat Management - Arista NG Firewall and Arista Micro Edge (Formerly Untangle)
- Arista NetVisor OS, Arista NetVisor UNUM, and Insight Analytics (Formerly Pluribus)
- VeloCloud Orchestrator (Formerly VeloCloud Orchestrator by Broadcom)
- VeloCloud Gateway (Formerly VeloCloud Gateway by Broadcom)
- VeloCloud Edge (Formerly VeloCloud Edge by Broadcom)

Note: certain software versions may not be supported on certain platforms

## Required Configuration for Exploitation

To be vulnerable to CVE-2026-2380, any of the following configurations must be present:

1. gNMI server is enabled
2. RESTCONF server is enabled
3. NETCONF server is enabled

With any of these servers enabled, the OpenConfig/Octa agent can log sensitive information in the local log file.

### OpenConfig agent sensitive logging (gNMI, NETCONF, RESTCONF)

#### gNMI

gNMI server is enabled, and a client sends a request with sensitive configuration.

```
#show running-config section gnmi
management api gnmi
   transport grpc default
```

or

#### RESTCONF

RESTCONF server is enabled, and a client sends a request with sensitive configuration.

```
#show running-config section restconf
management api restconf
   transport https default
      ssl profile mySslProfile
```

or

### NETCONF

NETCONF server is enabled, and a client sends a request with sensitive configuration.

```
#show running-config section netconf
management api netconf
   transport ssh default
```

In addition to local logging, sensitive information may be recorded on remote accounting servers if any of the following configurations are present:

### gRPC AAA accounting sensitive logging (for gNMI only)

The gNMI server is enabled with request accounting, and a client sends a request containing sensitive information.

```
#show running-config section gnmi
management api gnmi
   transport grpc default
      accounting requests
```

### gNSI.Acctz accounting sensitive logging (for gNMI only)

The gNMI server is enabled with gNSI.Acctz accounting, and a client sends a request with sensitive information.

```
#show running-config section gnmi
management api gnmi
   transport grpc default
#show running-config section gnsi
management api gnsi
   service acctz
```

### OpenConfig agent tracing sensitive logging

Requests containing sensitive configuration may be logged by default (i.e., without debug tracing enabled). However, enabling debug tracing for the OpenConfig/Octa agent may log additional sensitive information, such as responses and gNSI requests/responses.

OpenConfig agent with debug tracing enabled (at any level):

```
#show running-config section trace | grep OpenConfig
trace OpenConfig setting */*
```

Octa agent with debug tracing enabled (at any level):

```
#show running-config section trace | grep Octa
trace Octa setting */*
```

## Indicators of Compromise

Review logs for sensitive information. The specific data exposed depends on the services configured and whether requests contain sensitive information.

**Example:**

Consider a device with OpenConfig gNMI enabled. A gNMI.Set RPC with an **origin=cli** sensitive CLI command “**username bob secret myPass**” is issued. Consequently, the user password “**myPass**” is logged.

The OpenConfig/Octa agent logs in **/var/log/agents** may contain this sensitive command. Search for keywords relevant to your environment. A non-exhaustive example in this case “**secret**”.

In this case, the sensitive command can be searched with the following. The Octa agent name depends on whether “**provider eos-native**” is configured under “**management api gnmi**”.

```
switch# show agent OpenConfig logs | grep "secret"
```

```
switch# show agent Octa logs | grep "secret"
```

The sensitive command may appear in the agent logs as follows:

```
I0102 03:45:00.123456   12345 router.go:123] Cli commands:
enable
configure session session1234567890000
username bob secret myPass
end
configure session session1234567890000 commit
```

If additional debug logging is enabled, the request may also be logged as follows:

```
I0102 03:45:00.123456   12345 server.go:123] SetRequest: update: val:}
```

Additionally, suppose gNMI accounting logging is also configured to log with syslog.

In this case, the sensitive string can be searched as follows:

```
switch# show logging system | grep "secret"
```

The sensitive command may appear in syslog as follows:

```
<DATE> <HOST> Aaa: %ACCOUNTING-6-CMD: <RPC-CALLER> gRPC <ADDRESS> stop task_id=16 sta
rt_time=<TIME> timezone=PST service=shell priv-
lvl=0 cmd=OpenConfig.Set addr=<ADDRESS> rpc=/gnmi.gNMI/Set request=]} <cr>
```

Note that if TACACS+ or RADIUS is configured, this command may also be recorded on the remote accounting server.

## Mitigation

The vulnerability can be mitigated by avoiding the transmission of requests containing sensitive information over gNMI, RESTCONF, or NETCONF. Additionally, debug tracing for the OpenConfig or Octa agents should not be enabled, i.e., do not configure "**trace OpenConfig setting */***" or "**trace Octa setting */***"; please note that this can only avoid sensitive information showing in the debug traces, but can not mitigate the issue cause by other configurations mentioned in the Required Configuration for Exploitation section.

Should it be determined that sensitive information has been logged, the affected log files must

be truncated and any compromised secrets rotated to prevent unauthorized credential usage.

Use the following commands to clean up OpenConfig and Octa log files:

```
switch(config)# bash sudo truncate -s 0 /var/log/agents/OpenConfig*
switch(config)# bash sudo truncate -s 0 /var/log/agents/Octa*
```

Then use the following commands to clean up previously rotated old log files:

```
switch(config)# bash sudo find /var/log/agents -name 'OpenConfig*.gz' -type f -delete
switch(config)# bash sudo find /var/log/agents -name 'Octa*.gz' -type f -delete
```

## Resolution

The recommended resolution is to upgrade to a remediated software version at your earliest convenience. Arista recommends customers move to the latest version of each release that contains all the fixes listed below. For more information about upgrading see EOS User Manual: Upgrades and Downgrades

CVE-2026-2380 has been fixed in the following releases:

- 4.36.2F and later releases in the 4.36.x train

## Hotfix

No hotfix is available for this issue.

### For More Information

If you require further assistance, or if you have any further questions regarding this security notice, please contact the Arista Networks Technical Assistance Center (TAC) by one of the following methods:

### Open a Service Request

Contact information needed to open a new service request may be found at: https://www.arista.com/en/support/customer-support